More information about this series at http://www.springer.com/series/7410
Preface

The 20th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2017) was held March 28–31, 2017, in Amsterdam, The Netherlands. The conference is sponsored by the International Association for Cryptologic Research (IACR) and has an explicit focus on public-key cryptography.

These proceedings, consisting of two volumes, feature 36 papers; these were selected by the Program Committee from 160 qualified submissions. Each submission was reviewed independently by at least three reviewers, or four in the case of Program Committee member submissions. Following the initial reviewing phase, the submissions and their reviews were discussed over a period of one month, before final decisions were then made. During this discussion phase, the Program Committee made substantial use of a newer feature of the submission/review software, which allows direct yet anonymous communication between the Program Committee and the authors; I think this interaction proved very useful in resolving pending issues and questions.

The reviewing and selection process was an intensive and time-consuming task, and I thank the members of the Program Committee, along with the external reviewers, for all their hard work and their excellent job. I also want to acknowledge Shai Halevi for his awesome submission/review software, which tremendously simplifies the program chair’s work, and I thank him for his 24/7 and always-prompt assistance.

The conference program also included two invited talks, one by Vipul Goyal on “Recent Advances in Non-Malleable Cryptography,” and the other by Kenny Paterson on “The Evolution of Public Key Cryptography in SSL/TLS.” I would like to thank the two invited speakers as well as all the other speakers for their contributions to the program.

I also want to thank all the authors who submitted papers; you made it very challenging for the Program Committee to decide on what should be “the best” submissions — which of course is very much a matter of taste and perspective. I know that having good papers rejected because of a tough competition, and because there is always some amount of randomness involved, is disappointing, but I am optimistic that these “unlucky” papers will find their place and get the deserved recognition.

Last but not least, I would like to thank Marc Stevens, the general chair, for setting up a great conference and ensuring a smooth running of the event, and Ronald Cramer for his advisory support and allowing me to tap into his experience.

January 2017

Serge Fehr
PKC 2017

The 20th International Conference on Practice and Theory of Public-Key Cryptography

Amsterdam, The Netherlands
March 28–31, 2017

Sponsored by the
International Association of Cryptologic Research

General Chair
Marc Stevens CWI Amsterdam, The Netherlands

Program Chair
Serge Fehr CWI Amsterdam, The Netherlands

Program Committee
Masayuki Abe NTT Secure Platform Labs, Japan
Fabrice Benhamouda IBM Research, USA
Nir Bitansky MIT, USA
Zvika Brakerski Weizmann Institute of Science, Israel
Nishanth Chandran Microsoft Research, India
Dana Dachman-Soled University of Maryland, USA
Nico Döttling UC Berkeley, USA
Léo Ducas CWI Amsterdam, The Netherlands
Sebastian Faust Ruhr-University Bochum, Germany
Dario Fiore IMDEA Software Institute, Spain
Pierre-Alain Fouque Rennes 1 University, France
Georg Fuchsbauer ENS, France
Sanjam Garg UC Berkeley, USA
Jens Groth University College London, UK
Carmit Hazay Bar-Ilan University, Israel
Dennis Hofheinz KIT, Germany
Tibor Jager Paderborn University, Germany
Abhishek Jain Johns Hopkins University, USA
Marcel Keller University of Bristol, UK
Markulf Kohlweiss Microsoft Research, UK
Vadim Lyubashevsky IBM Research Zurich, Switzerland
Takahiro Matsuda  
AIST, Japan

Adam O’Neill  
Georgetown University, USA

Arpita Patra  
Indian Institute of Science, India

Ludovic Perret  
Sorbonnes University, UPMC/Inria/CNRS, France

Christophe Petit  
University of Oxford, UK

Vanishree Rao  
PARC, USA

Alessandra Scafuro  
North Carolina State University, USA

Gil Segev  
Hebrew University of Jerusalem, Israel

Fang Song  
Portland State University, USA

Daniele Venturi  
Sapienza University of Rome, Italy

Hoeteck Wee  
ENS, France

Vassilis Zikas  
Rensselaer Polytechnic Institute, USA

**External Reviewers**

Hamza Abusalah  
Mahdi Cheraghchi  
Kristina Hostakova

Shashank Agrawal  
Céline Chevalier  
Vincenzo Iovino

Tristan Allard  
Seung Geol Choi  
Malika Izabache

Miguel Ambrona  
Arka Rai Choudhary  
Sune Jakobsen

Daniel Apon  
Kai-Min Chung  
Marc Joye

Diego F. Aranha  
Aloni Cohen  
Charanjit Jutla

Nuttapong Attrapadung  
Sandro Coretti  
Ali El Kaafarani

Christian Badertscher  
Véronique Cortier  
Bhavana Kanukurthi

Saikrishna Badrinarayanan  
Anamaria Costache  
Koray Karabina

Shi Bai  
Geoffroy Couteau  
Aniket Kate

Foteini Baldimtsi  
Lisa Eckey  
Dakshita Khurana

Marshall Ball  
Antonio Faonio  
Eike Kiltz

Carsten Baum  
Luca di Feo  
Taechan Kim

David Bernhard  
Tore Kasper Frederiksen  
Elena Kirshanova

Silvio Biagioni  
Tommaso Gagliardoni  
Fuyuki Kitagawa

Jean-Francois Biasse  
Steven Galbraith  
Yutaro Kiyomura

Olivier Blazy  
David Galindo  
Susumu Kiyoshima

Jonathan Bootle  
Pierrick Gaudry  
Lisa Kohl

Joppe Bos  
Romain Gay  
Ilan Komargodski

Cecilia Boschini  
Marilyn George  
Yashvanth Kondi

Florian Bourse  
Essam Ghadafi  
Venkata Koppula

Elette Boyle  
Junqing Gong  
Luke Kowalczyk

Chris Brzuska  
Aurore Guillevic  
Juliane Krämer

Angelo De Caro  
Felix Günther  
Mukul Kulkarni

Wouter Castryck  
Ryo Hiromasa  
Thijs Laarhoven

Dario Catalano  
Mohammad Hajiabadi  
Sebastian Lauer

Andrea Cerulli  
Yoshikazu Hanatani  
Moon Sung Lee

Pyrros Chaidos  
Ethan Heilman  
Tancredè Lepoint

Jie Chen  
Justin Holmgren  
Qinyi Li
Benoît Libert
Satyanarayana Lokam
Patrick Longa
Steve Lu
Yun Lu
Bernardo Magri
Mary Maller
Alex Malozemoff
Antonio Marcedone
Giorgia Azzurra Marson
Daniel Masny
Nicolas Meloni
Peihan Miao
Giacomo Micheli
Michele Minelli
Ameeer Mohammed
Pratyay Mukherjee
Debdeep Mukhopadhyay
Patrick Märtens
Pierrick Méaux
Michael Naehrig
Gregory Neven
Anca Nitulescu
Luca Nizzardo
Ariel Nof
Koji Nuida
Maciej Obremski
Miyako Ohkubo
Cristina Onete
Michele Orrù
Daniel Page
Jiaxin Pan
Dimitris Papadopoulos
Sunoo Park
Anat Paskin-Cherniavsky
Alain Passelègue
Valerio Pastro
Cécile Pierrot
Rafael del Pino
Rachel Player
Oxana Poburinnaya
David Pointcheval
Antigoni Polychroniadou
Manoj Prabhakaran
Benjamin Pring
Srinivasan Raghuraman
Joost Renes
Răzvan Rosie
Dragos Rotaru
Tim Ruffing
Akshayaram Srinivasan
Yusuke Sakai
Kazuo Sakiyama
John M. Schanck
Benedikt Schmidt
Peter Scholl
Jacob Schuldt
Peter Schwabe
Sven Schäge
Ido Shahaf
Igor Shparlinski
Shashank Singh
Luisa Siniscalchi
Ben Smith
Douglas Stebila
Kim Taechan
Atsushi Takayasu
Vanessa Teague
Adrien Thillard
Aishwarya
Thiruvenkadam
Yan Bo Ti
Mehdi Tibouchi
Junichi Tomida
Daniel Tschudi
Dominique Unruh
Alexander Ushakov
Satyanarayana Vusirikala
Xiao Wang
Yohei Watanabe
Avi Weinstock
Mor Weiss
David Wu
Keita Xagawa
Shota Yamada
Takashi Yamakawa
Avishek Yanai
Eylon Yogev
Kazuki Yoneyama
Yang Yu
Mark Zhandry
Jean Karim Zinzindohoué
Michael Zohner
Contents – Part I

Cryptanalysis

LP Solutions of Vectorial Integer Subset Sums – Cryptanalysis
of Galbraith’s Binary Matrix LWE ...................................................... 3
  Gottfried Herold and Alexander May

Improved Algorithms for the Approximate $k$-List Problem
in Euclidean Norm ................................................................. 16
  Gottfried Herold and Elena Kirshanova

Zeroizing Attacks on Indistinguishability Obfuscation over CLT13 ........ 41
  Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint,
  and Mehdi Tibouchi

Protocols

Cut Down the Tree to Achieve Constant Complexity in Divisible E-cash..... 61
  David Pointcheval, Olivier Sanders, and Jacques Traoré

Asymptotically Tight Bounds for Composing ORAM with PIR ............. 91
  Ittai Abraham, Christopher W. Fletcher, Kartik Nayak, Benny Pinkas,
  and Ling Ren

Predictable Arguments of Knowledge ........................................... 121
  Antonio Faonio, Jesper Buus Nielsen, and Daniele Venturi

Removing Erasures with Explainable Hash Proof Systems ................ 151
  Michel Abdalla, Fabrice Benhamouda, and David Pointcheval

Scalable Multi-party Private Set-Intersection .................................. 175
  Carmit Hazay and Muthuramakrishnan Venkitasubramaniam

Encryption Schemes

Tightly Secure IBE Under Constant-Size Master Public Key ............... 207
  Jie Chen, Junqing Gong, and Jian Weng

Separating IND-CPA and Circular Security for Unbounded Length
Key Cycles ................................................................. 232
  Rishab Goyal, Venkata Koppula, and Brent Waters
Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts ........................................ 247
Benoît Libert, Thomas Peters, and Chen Qian

Leakage-Resilient and Non-Malleable Codes

Non-malleable Codes with Split-State Refresh .......................... 279
Antonio Faonio and Jesper Buus Nielsen

Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-malleable Codes ...................... 310
Dana Dachman-Soled, Mukul Kulkarni, and Aria Shahverdi

Fully Leakage-Resilient Codes .............................................. 333
Antonio Faonio and Jesper Buus Nielsen

Number Theory and Diffie-Hellman

On the Bit Security of Elliptic Curve Diffie–Hellman .................. 361
Barak Shani

Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree .................... 388
Taechan Kim and Jinhyuck Jeong

Provably Secure NTRU Instances over Prime Cyclotomic Rings .... 409
Yang Yu, Guangwu Xu, and Xiaoyun Wang

Equivalences and Black-Box Separations of Matrix Diffie-Hellman Problems ......................................................... 435
Jorge L. Villar

Author Index ................................................................. 465
## Contents – Part II

### Encryption with Access Control

**Dual System Framework in Multilinear Settings and Applications to Fully Secure (Compact) ABE for Unbounded-Size Circuits.**

_Nuttapong Attrapadung_  
3

**CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions.**

_Fabrice Benhamouda, Florian Bourse, and Helger Lipmaa_

36

**Bounded-Collusion Attribute-Based Encryption from Minimal Assumptions.**

_Gene Itkis, Emily Shen, Mayank Varia, David Wilson, and Arkady Yerukhimovich_

67

**Access Control Encryption for Equality, Comparison, and More.**

_Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, and Claudio Orlandi_

88

### Special Signatures

**Deterring Certificate Subversion: Efficient Double-Authentication-Preventing Signatures.**

_Mihir Bellare, Bertram Poettering, and Douglas Stebila_

121

**Chameleon-Hashes with Ephemeral Trapdoors: And Applications to Invisible Sanitizable Signatures.**

_Jan Camenisch, David Derler, Stephan Krenn, Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig_

152

**Improved Structure Preserving Signatures Under Standard Bilinear Assumptions.**

_Charanjit S. Jutla and Arnab Roy_

183

### Fully Homomorphic Encryption

**Chosen-Ciphertext Secure Fully Homomorphic Encryption.**

_Ran Canetti, Srinivasan Raghuraman, Silas Richelson, and Vinod Vaikuntanathan_

213

**Circuit-Private Multi-key FHE.**

_Wutichai Chongchitmate and Rafail Ostrovsky_

241
FHE over the Integers: Decomposed and Batched in the Post-Quantum Regime .................................................. 271
   Daniel Benarroch, Zvika Brakerski, and Tancrède Lepoint

Real-World Schemes

Ceremonies for End-to-End Verifiable Elections .......................... 305
   Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang

A Modular Security Analysis of EAP and IEEE 802.11 .................. 335
   Chris Brzuska and Håkon Jacobsen

Multiparty Computation

On the Computational Overhead of MPC with Dishonest Majority .... 369
   Jesper Buus Nielsen and Samuel Ranellucci

Better Two-Round Adaptive Multi-party Computation .................. 396
   Ran Canetti, Oxana Poburinnaya, and Muthuramakrishnan Venkitasubramaniam

Constant Round Adaptively Secure Protocols in the Tamper-Proof Hardware Model ............................................. 428
   Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam

Primitives

Constrained Pseudorandom Functions for Unconstrained Inputs Revisited: Achieving Verifiability and Key Delegation ....................... 463
   Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay

Constraining Pseudorandom Functions Privately .......................... 494
   Dan Boneh, Kevin Lewi, and David J. Wu

Universal Samplers with Fast Verification ................................. 525
   Venkata Koppula, Andrew Poelstra, and Brent Waters

Author Index ........................................................................ 555